Journal of Mathematical Physics, Analysis, Geometry
2013, vol. 9, No. 4, pp. 582–593

On the Skitovich–Darmois Theorem for $\boldsymbol{a}$-Adic Solenoids

I.P. Mazur

B. Verkin Institute for Low Temperature Physics and Engineering
National Academy of Sciences of Ukraine
47 Lenin Ave., Kharkiv 61103, Ukraine
E-mail: mazurivan85@gmail.com

Received July 10, 2013

By the Skitovich–Darmois theorem, the Gaussian distribution on the real line is characterized by the independence of two linear forms of n independent random variables. The theorem is known to fail for a compact connected Abelian group even in the case when $n = 2$. In the paper, it is proved that a weak analogue of the Skitovich–Darmois theorem holds for some $\boldsymbol{a}$-adic solenoids if we consider three independent linear forms of three random variables.

Key words: Skitovich–Darmois theorem, functional equation, $\boldsymbol{a}$-adic solenoid.

Mathematics Subject Classification 2010: 39B52, 62E10, 60B15.

1. Introduction

It is well known that the proofs of many characterization theorems of mathematical statistics are reduced to the solving of some functional equations. Consider the classical Skitovich–Darmois theorem that characterizes Gaussian distributions on the real line ([9, Ch. 3]): Let $\xi_i, i = 1, 2, \ldots, n$, $n \geq 2$, be independent random variables, and α_j, β_j be nonzero constants. Suppose that the linear forms $L_1 = \alpha_1\xi_1 + \cdots + \alpha_n\xi_n$ and $L_2 = \beta_1\xi_1 + \cdots + \beta_n\xi_n$ are independent. Then all random variables ξ_j are Gaussian.

Let $\hat{\mu}_j(y)$ be the characteristic functions of the distributions of ξ_j, $j = 1, 2, \ldots, n$. Taking into account that $\mathbf{E}[e^{i\xi_j y}] = \hat{\mu}_j(y)$, it is easy to verify that the Skitovich–Darmois theorem is equivalent to the following statement: The

This research was conducted in the frames of the project "Ukrainian Branch of the French-Russian Poncelet Laboratory" - "Probability Problems on Groups and Spectral Theory" and was supported in part by the grant ANR-09-BLAN-0084-01 and by the scholarship of French Embassy in Ukraine.

solutions of the Skitovich–Darmois equation

$$\prod_{j=1}^{n} \hat{\mu}_j(\alpha_j u + \beta_j v) = \prod_{j=1}^{n} \hat{\mu}_j(\alpha_j u)\hat{\mu}_j(\beta_j v), \quad u, v \in \mathbb{R},$$

in the class of the normalized continuous positive definite functions are the characteristic functions of the Gaussian distributions, i.e., $\hat{\mu}_j(y) = \exp\{ia_j y - \sigma_j y^2\},\ a_j \in \mathbb{R}, \sigma_j \geq 0, y \in \mathbb{R},\ j = 1, 2, \ldots, n.$

This theorem was generalized to various classes of locally compact Abelian groups (see, for example, [1–6], [10]). In these researches random variables take values in a locally compact Abelian group X, and coefficients of the linear forms are topological automorphisms of X. As in the classical case, the characterization problem is reduced to the solving of the Skitovich–Darmois equation in the class of the normalized continuous positive definite functions on the character group of the group X.

In [2], G.M. Feldman and P. Graczyk showed that even a weak analogue of the Skitovich–Darmois theorem fails for compact connected Abelian groups. Namely, they proved the following statement: Let X be an arbitrary compact connected Abelian group. Then there exist topological automorphisms $\alpha_j, \beta_j, j = 1, 2,$ of X and independent random variables ξ_1, ξ_2 with values in X and distributions that are not convolutions of the Gaussian and idempotent distributions, whereas the linear forms $L_1 = \alpha_1\xi_1 + \alpha_2\xi_2$ and $L_2 = \beta_1\xi_1 + \beta_2\xi_2$ are independent.

The aim of this article is to show that a weak analogue of the Skitovich–Darmois theorem holds for some compact connected Abelian groups if we consider three linear forms of three random variables. Namely, we will construct an $\boldsymbol{a}$-adic solenoid $\Sigma_{\boldsymbol{a}}$ (the full description of these solenoids will be given in Theorem 4.1) for which the independence of three linear forms of three independent random variables with values in $\Sigma_{\boldsymbol{a}}$ implies that at least one random variable has an idempotent distribution.

2. Definitions and Notation

Let X be a second countable locally compact Abelian group. Denote by $Aut(X)$ the group of the topological automorphisms of X. Let k be an integer. Denote by f_k the mapping $f_k : X \to X$ defined by the equality $f_k x = kx$. Put $X^{(k)} = f_k(X)$.

Let $Y = X^*$ be the character group of X. The value of a character $y \in Y$ at $x \in X$ denote by (x, y). Let B be a nonempty subset of X. Put

$$A(Y, B) = \{y \in Y : (x, y) = 1, x \in B\}.$$

The set $A(Y, B)$ is called the annihilator of B in Y. The annihilator $A(Y, B)$ is a closed subgroup in Y. For each $\alpha \in Aut(X)$ define the mapping $\tilde{\alpha} : Y \to Y$ by the equality $(\alpha x, y) = (x, \tilde{\alpha} y)$ for all $x \in X, y \in Y$. The mapping $\tilde{\alpha}$ is a topological automorphism of Y. It is called an adjoint of α. The identity automorphism of a group X denote by I.

In the paper, we will use standard facts of abstract harmonic analysis (see [12]). Let μ be a distribution on X. The characteristic function of μ is defined by the formula

$$\hat{\mu}(y) = \int\limits_X (x, y) d\mu(y), y \in Y.$$

Put $F_\mu = \{y \in Y : \hat{\mu}(y) = 1\}$. Then F_μ is a subgroup of Y, and the function $\hat{\mu}(y)$ is F_μ-invariant, i.e., $\hat{\mu}(y + h) = \hat{\mu}(y), y \in Y, h \in F_\mu$.

Denote by E_x the degenerate distribution concentrated at x. Let K be a compact subgroup of X. Denote by m_K the Haar distribution on K. Denote by $I(X)$ the set of shifts of these distributions, i.e., the distributions of the form $m_K * E_x$, where K is a compact subgroup of X, $x \in X$. The distributions of the class $I(X)$ are called idempotent. Note that the characteristic function of m_K is of the form

$$\hat{m}_K(y) = \begin{cases} 1, & y \in A(Y, K), \\ 0, & y \notin A(Y, K). \end{cases}$$

A distribution μ on the group X is called Gaussian ([13], ch. 5) if its characteristic function can be represented in the form

$$\hat{\mu}(y) = (x, y) \exp\{-\varphi(y)\}, \quad y \in Y,$$

where $\varphi(y)$ is a continuous nonnegative function satisfying the equation

$$\varphi(u + v) + \varphi(u - v) = 2(\varphi(u) + \varphi(v)), \quad u, v \in Y.$$

Denote by $\Gamma(X)$ the set of Gaussian distributions on X.

Denote by $\mathbb{Z}$ the infinite cyclic group, by $\mathbb{R}$ the additive group of real numbers, by $\mathbb{T}$ the circle group, by $\mathbb{Q}$ the additive group of rational numbers with the discrete topology, by $\Delta_{\boldsymbol{a}}$ the group of $\boldsymbol{a}$-adic integers, by $\mathbb{Z}(m)$ the group of residue modulo m.

Let $\boldsymbol{a} = (a_0, a_1, \ldots, a_n, \ldots)$ be a fixed but arbitrary infinite sequence of natural numbers, where all $a_i > 1$. Consider the group $\mathbb{R} \times \Delta_{\boldsymbol{a}}$. Let B be a subgroup of $\mathbb{R} \times \Delta_{\boldsymbol{a}}$ of the form $B = \{(n, n\mathbf{u})\}_{n=-\infty}^{\infty}$, where $\mathbf{u} = (1, 0, \ldots, 0, \ldots)$. The factor-group $\boldsymbol{\Sigma}_{\boldsymbol{a}} = (\mathbb{R} \times \Delta_{\boldsymbol{a}})/B$ is called an $\boldsymbol{a}$-adic solenoid. The group $\boldsymbol{\Sigma}_{\boldsymbol{a}}$ is a compact connected Abelian group having dimension 1. Moreover, $\boldsymbol{\Sigma}_{\boldsymbol{a}}^* \cong H_{\boldsymbol{a}}$, where

$$H_{\boldsymbol{a}} = \{\frac{m}{a_0 a_1 \cdots a_n} : n = 0, 1, \ldots; m \in \mathbb{Z}\}$$

is a subgroup of $\mathbb{Q}$. Denote by $\mathcal{P}$ the set of prime numbers.

3. Lemmas

Let X be a locally compact Abelian group. Put $Y = X^*$, $\tilde{\alpha}_{ij} \in Aut(Y), i, j = 1, 2, \dots, n$. Let $f_i(y)$ be some functions on Y. Recall that the Skitovich–Darmois equation is an equation of the form

$$\prod_{i=1}^{n} f_i\left(\sum_{j=1}^{n} \tilde{\alpha}_{ij} u_j\right) = \prod_{i=1}^{n}\prod_{j=1}^{n} f_i(\tilde{\alpha}_{ij} u_j), \quad u_j \in Y. \tag{1}$$

The proof of the main theorem is reduced to the studying of the solutions of this equation. In order to prove the main result, we need some lemmas.

Lemma 3.1. ([11]). *Let X be a second countable locally compact Abelian group, $\xi_i, i = 1, 2, \dots, n$, be independent random variables with values in X and distributions μ_i. The linear forms $L_j = \sum_{i=1}^{n} \alpha_{ij}\xi_i, j = 1, 2, \dots, n$, where $\alpha_{ij} \in Aut(X)$, are independent if and only if the characteristic functions $\hat{\mu}_i(y), i = 1, 2, \dots, n$, satisfy equation (1), which takes the form*

$$\prod_{i=1}^{n} \hat{\mu}_i\left(\sum_{j=1}^{n} \tilde{\alpha}_{ij} u_j\right) = \prod_{i=1}^{n}\prod_{j=1}^{n} \hat{\mu}_i(\tilde{\alpha}_{ij} u_j), \quad u_j \in Y. \tag{2}$$

Lemma 3.2. ([11]). *Let X be a direct product of the groups $\mathbb{Z}(p^{k_p})$, where $k_p \geq 0$, i.e., $X = \mathbf{P}_{p\in\mathcal{P}}\mathbb{Z}(p^{k_p})$. Let $\xi_i, i = 1, 2, \dots, n$, be independent random variables with values in X and distributions μ_i. Then the independence of the linear forms $L_j = \sum_{i=1}^{n} \alpha_{ij}\xi_i$, where $\alpha_{ij} \in Aut(X), \alpha_{1j} = \alpha_{i1} = I, i, j = 1, 2, \dots, n$, implies that $\mu_i = E_{x_i} * m_K$, where K is a compact subgroup of X, $x_i \in X$, $i = 1, 2, \dots, n$.*

Taking into account that $X = \mathbf{P}_{p\in\mathcal{P}}\mathbb{Z}(p^{k_p})$ if and only if Y is a weak direct product of the groups $\mathbb{Z}(p^{k_p})$, where $k_p \geq 0$, i.e., $Y = \mathbf{P}^*_{p\in\mathcal{P}}\mathbb{Z}(p^{k_p})$, by Lemmas 3.1 and 3.2 we obtain

Corollary 3.3. *Let Y be a discrete Abelian group of the form $Y = \mathbf{P}^*_{p\in\mathcal{P}}\mathbb{Z}(p^{k_p})$, where $k_p \geq 0$. Let $\hat{\mu}_i(y), i = 1, 2, \dots, n$, $n \geq 2$, be the characteristic functions on Y satisfying Eq.* (2)*, where $\tilde{\alpha}_{ij} \in Aut(Y), \tilde{\alpha}_{1j} = \tilde{\alpha}_{i1} = I, i, j = 1, 2, \dots, n$. Then $\hat{\mu}_i(y) = (x_i, y)\hat{m}_K(y), y \in Y$, where K is a compact subgroup of X, $x_i \in X$, $i = 1, 2, \dots, n$.*

The following lemma states that an analogue of the Skitovich–Darmois theorem for three linear forms of three independent random variables holds on the circle group if we assume that the characteristic functions of the random variables do not vanish.

Lemma 3.4. ([8]) *Assume that* $X = \mathbb{T}, \alpha_{ij} \in Aut(X), i, j = 1, 2, 3$. *Let* $\xi_i, i = 1, 2, 3$, *be independent random variables with values in* X *and distributions* μ_i *such that their characteristic functions do not vanish. Suppose that* $L_j = \sum_{i=1}^{3} \alpha_{ij}\xi_i, j = 1, 2, 3$, *are independent. Then* $\mu_i = E_{x_i}$, $x_i \in X$, $i = 1, 2, 3$.

By Lemmas 3.1 and 3.4, we obtain

Corollary 3.5. *Assume that* $Y = \mathbb{Z}$. *Let* $\hat{\mu}_i(y), i = 1, 2, 3$, $n \geq 2$, *be non-vanishing characteristic functions on* Y *satisfying the equation*

$$\hat{\mu}_1(u_1 + u_2 + u_3)\hat{\mu}_2(u_1 - u_2 - u_3)\hat{\mu}_3(u_1 + u_2 - u_3)$$
$$= \hat{\mu}_1(u_1)\hat{\mu}_1(u_2)\hat{\mu}_1(u_3)\hat{\mu}_2(u_1)\hat{\mu}_2(-u_2)\hat{\mu}_2(-u_3)\hat{\mu}_3(u_1)\hat{\mu}_3(u_2)\hat{\mu}_3(-u_3),$$
$$u_i \in Y, i = 1, 2, 3. \tag{3}$$

Then $\hat{\mu}_i(y) = (x_i, y), x_i \in X, i = 1, 2, 3, y \in Y$.

The following lemma for the case $n = 2$ has been proved earlier (see, for example, [7], Lemma 13.20). The proof for the arbitrary n is almost the same.

Lemma 3.6. *Let* X *be a second countable compact Abelian group. Suppose that there exists an automorphism* $\delta \in Aut(X)$ *and an element* $\tilde{y} \in Y$ *such that the following conditions are satisfied:*

i) $Ker(I - \tilde{\delta}) = \{0\}$;

ii) $(I - \tilde{\delta})Y \cap \{0; \pm\tilde{y}, \pm 2\tilde{y}\} = \{0\}$;

iii) $\tilde{\delta}\tilde{y} \neq -\tilde{y}$.

Then for all $n \geq 2$ *there exist independent identically distributed random variables* $\xi_i, i = 1, 2, \ldots, n$, *with values in* X *and distribution* $\mu \notin I(X) * \Gamma(X)$ *such that the linear forms* $L_j = \xi_1 + \sum_{i=2}^{n} \delta_{ij}\xi_i, j = 1, 2, \ldots, n$, *where* $\delta_{ij} = I, i \neq j, \delta_{ii} = \delta$, *are independent.*

It is convenient for us to formulate the following simple statement as a lemma.

Lemma 3.7. *Let* Y *be a second countable discrete Abelian group,* H *be a subgroup of* Y, *and* $f(y)$ *be a function on* Y *of the form*

$$f(y) = \begin{cases} 1, & y \in H; \\ c, & y \notin H, \end{cases} \tag{4}$$

where $0 < c < 1$. *Then* $f(y)$ *is a positive definite function.*

P r o o f. Consider the distribution $\mu = cE_0 + (1 - c)m_G$ on the group X, where $G = A(X, H)$. It is easy to see that $f(y) = \hat{\mu}(y)$. Hence, $f(y)$ is a positive definite function. ∎

The following lemma for $n = 2$ was proved in [2].

Lemma 3.8. *Let X be a second countable compact connected Abelian group such that $f_2 \in Aut(X)$. Then there exist independent random variables $\xi_i, i = 1, 2, \ldots, n$, with values in X and distributions $\mu_i \notin I(X) * \Gamma(X)$, and automorphisms $\alpha_{ij} \in Aut(X)$ such that the linear forms $L_j = \sum_{i=1}^n \alpha_{ij}\xi_i, j = 1, 2, \ldots, n$, are independent.*

P r o o f. There are two cases possible:
1. $f_p \in Aut(X)$ for all prime numbers p;
2. $f_p \notin Aut(X)$ for a prime number p.

1. Consider the first case. It is well known that if X is a compact Abelian group X such that $f_p \in Aut(X)$ for all prime p, then

$$X \cong (\boldsymbol{\Sigma_a})^{\mathfrak{n}}, \tag{5}$$

where $\boldsymbol{a} = (2, 3, 4, \ldots)$, ([12, (25.8)]). It is obvious that it suffices to prove the lemma for the group of the form $X = \boldsymbol{\Sigma_a}, \boldsymbol{a} = (2, 3, 4, \ldots)$. Then the group Y is topologically isomorphic to the group $\mathbb{Q}$. Let p and q be different prime numbers. Let H be a subgroup of Y of the form $H = \{\frac{m}{q^k}\}_{m,k\in\mathbb{Z}}$. Put $G = H^*, K = A(G, H^{(p)})$. Since the numbers p and q are relatively prime, it follows that $H \neq H^{(p)}$. On the group H, consider the function

$$f(y) = \begin{cases} 1, & y \in H^{(p)}, \\ c, & y \notin H^{(p)}, \end{cases} \tag{6}$$

where $0 < c < 1$. By Lemma 3.7, $f(y)$ is a positive definite function.

On the group Y, consider the function

$$g(y) = \begin{cases} f(y), & y \in H, \\ 0, & y \notin H. \end{cases} \tag{7}$$

The function $g(y)$ is a positive definite function ([7, Theorem 2.12]). By the Bohner theorem, there exists a distribution $\mu \in M^1(X)$ such that $\hat{\mu}(u) = g(y)$. It is obvious that $\mu \notin I(X) * \Gamma(X)$.

Let ξ_i be independent random variables with values in X and distribution μ. Put $s = p^2 + q$. From the conditions of the lemma it follows that $s \in Aut(X)$. Let us show that the linear forms

$$L_1 = \xi_1 + p\xi_2 + p\xi_3 + \cdots + p\xi_n,$$

$$L_2 = p\xi_1 + s\xi_2 + p^2\xi_3 + \cdots + p^2\xi_n,$$

$$L_3 = p\xi_1 + p^2\xi_2 + s\xi_3 + \cdots + p^2\xi_n,$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$L_n = p\xi_1 + p^2\xi_2 + p^2\xi_3 + \cdots + s\xi_n$$

are independent. By Lemma 3.1, it suffices to show that there holds the following equation:

$$\hat{\mu}(u_1 + pu_2 + pu_3 + \cdots + pu_n)\hat{\mu}(pu_1 + su_2 + p^2u_3 + \cdots + p^2u_n) \times \cdots$$
$$\times\hat{\mu}(pu_1 + p^2u_2 + \cdots + su_n) = \hat{\mu}(u_1)\hat{\mu}(pu_2)\hat{\mu}(pu_3)\cdots\hat{\mu}(su_n). \tag{8}$$

From (6), it follows that

$$g(y + pt) = g(y), \quad y, t \in H. \tag{9}$$

Using (9), it is easy to show that if $u_i \in H$, then Eq. (8) becomes an equality. Thus it suffices to consider the case where $u_i \notin H$ for some i. It is easy to see that in this case the right-hand side of Eq. (8) vanishes.

Let us show that the left-hand side of Eq. (8) vanishes too. Assume the converse, i.e., that the left-hand side of Eq. (8) does not vanish. Then there holds the following system of equations:

$$\begin{cases} u_1 + pu_2 + pu_3 + \ldots + pu_n = h_1, \\ pu_1 + su_2 + p^2u_3 + \ldots + p^2u_n = h_2, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ pu_1 + p^2u_2 + p^2u_3 + \ldots + su_n = h_n, \end{cases} \tag{10}$$

where $h_i \in H$.

Add the first equation of the system (10) multiplied by $(-p)$ to each equation of the system (10) starting from the second one. We obtain that $qu_i = h_i - ph_1, i = 2, 3, \ldots, n$. Thus, $u_i \in H, i = 2, 3, \ldots, n$. From this and from the first equation of the system (10) it follows that that $u_1 \in H$. Finally we obtain that $u_i \in H, i = 1, 2, \ldots, n$, which contradicts the assumption.

2. Assume that

$$f_p \notin Aut(X) \tag{11}$$

for some prime number p. Suppose that p is the smallest natural number satisfying condition (11). Since X is a connected group, we have $X^{(n)} = X$ for all natural n. Hence, if $f_p \notin Aut(X)$, then $Ker f_p \neq \{0\}$.

From the condition of the lemma it follows that $p \geq 3$. Put $a = 1 - p$. Since p is the smallest natural number satisfying condition (11), we obtain $f_{-a} \in Aut(X)$. Hence $f_a \in Aut(X)$. Note that $Ker f_p = A(X, Y^{(p)})$. It implies that $Y^{(p)} \neq Y$. Let $\tilde{y} \in Y^{(p)}$ and verify that the automorphism $\delta = f_a$ and the element $\tilde{y}$ satisfy the conditions of Lemma 3.6. We have $\tilde{f}_a = f_a$ and $I - \tilde{f}_a = \tilde{f}_p$. Since Y is a torsion-free group, it follows that $Ker(I - \tilde{f}_a) = \{0\}$, i.e., condition (i) holds. Thus $(I - \tilde{f}_a)Y = Y^{(p)}$. From $p \geq 3$, it follows that the numbers 2 and p are relatively prime. Hence there are the integers m and n such that $2m + pn = 1$. Thus $y = 2my + pny$. Therefore, if $\tilde{y} \notin Y^{(p)}$, then $2\tilde{y} \notin Y^{(p)}$ too. It implies that condition (ii) holds. Taking into account that Y is a torsion-free group, it is obvious that condition (iii) holds. We use Lemma 3.6 to obtain the assertion of the lemma. ∎

4. Main Theorem

Theorem 4.1. *Let $X = \boldsymbol{\Sigma_a}$ be an $\boldsymbol{a}$-adic solenoid.*

1. *Assume that $f_p \notin Aut(X)$ for all prime numbers p. Let $\xi_i, i = 1, 2, 3,$ be independent random variables with values in X and distributions μ_i. Then the independence of the linear forms $L_j = \sum_{i=1}^{3} \alpha_{ij}\xi_i$, where $\alpha_{ij} \in Aut(X), i, j = 1, 2, 3,$ implies that at least one distribution $\mu_i \in I(X)$.*

2. *Assume that $f_p \in Aut(X)$ for a prime number p. Then there are independent random variables $\xi_i, i = 1, 2, 3,$ with values in X and distributions $\mu_i \notin \Gamma(X) * I(X)$, and automorphisms $\alpha_{ij} \in Aut(X)$ such that the linear forms $L_j = \sum_{i=1}^{3} \alpha_{ij}\xi_i, j = 1, 2, 3,$ are independent.*

It should be noted that an example of a group such that $f_p \notin Aut(X)$ for all prime numbers p is the group $\boldsymbol{\Sigma_a}, \boldsymbol{a} = (2, 3, 5, 7, \ldots)$. Its character group is $\boldsymbol{\Sigma}^*_{\boldsymbol{a}} \cong \{\frac{m}{p_1 p_2 \cdots p_k} : m \in \mathbb{Z}$, where p_j are different prime numbers$\}$.

An example of a group such that $f_p \in Aut(X)$ for a prime number p is the group $\boldsymbol{\Sigma_a}, \boldsymbol{a} = (2, 2, 2 \ldots)$. Its character group is $\boldsymbol{\Sigma}^*_{\boldsymbol{a}} \cong \{\frac{m}{2^k} : m, k \in \mathbb{Z}\}$.

The proof of Theorem 4.1 is divided into two parts. In the first part we use Corollaries 3.3 and 3.5. In the second part we use Lemma 3.8.

P r o o f. **1**. Suppose that $f_p \notin Aut(X)$ for all prime numbers p. This implies that $Aut(X) = \{I, -I\}$. It is easy to show that the case of arbitrary linear forms L_j is reduced to the case where L_j are of the form

$$
\begin{aligned}
L_1 &= \xi_1 + \xi_2 + \xi_3, \\
L_2 &= \xi_1 - \xi_2 + \xi_3, \\
L_3 &= \xi_1 - \xi_2 - \xi_3.
\end{aligned} \tag{12}
$$

Note that Y is topologically isomorphic to a subgroup of $\mathbb{Q}$. To avoid introducing new notation, we will suppose that Y is a subgroup of $\mathbb{Q}$. By Lemma 3.1, the independence of the linear forms (12) implies that Eq. (3), where Y is a subgroup of $\mathbb{Q}$, holds.

Note that since $f_2 \notin Aut(X)$, we have that the partition of Y into the cosets of $Y^{(2)}$ consists of two cosets: $Y^{(2)}$ and $\tilde{y} + Y^{(2)}$, where $\tilde{y} \notin Y^{(2)}$.

Put $N_i = \{y \in Y : \hat{\mu}_i(y) \neq 0\}, N = \cap_{i=1}^3 N_i$. We infer from (3) that N is a subgroup in Y. Moreover, it is easy to see from (3) that N has a property:

$$\text{if } 2y \in N, \text{ then } y \in N. \tag{13}$$

There are two cases: $N \neq \{0\}$ and $N = \{0\}$.

A. Assume that $N \neq \{0\}$. Suppose that t_1 and t_2 belong to the same coset of $Y^{(2)}$ in Y. Then there exists $\hat{u}_1$ and $\hat{u}_2$ such that $\hat{u}_1 + \hat{u}_2 = t_1, \hat{u}_1 - \hat{u}_2 = t_2$. Putting first $u_1 = \hat{u}_1, u_2 = \hat{u}_2, u_3 = 0$ in (3), then $u_1 = \hat{u}_1, u_2 = -\hat{u}_2, u_3 = 0$ in (3), and equating the right-hand sides of the obtained equations, we get

$$|\hat{\mu}_1(t_1)||\hat{\mu}_2(t_2)||\hat{\mu}_3(t_1)| = |\hat{\mu}_1(t_2)||\hat{\mu}_2(t_1)||\hat{\mu}_3(t_2)|.$$

Reasoning in the same way, it is easy to see that if t_1 and t_2 belong to the same coset of $Y^{(2)}$ in Y, then there holds the equation

$$|\hat{\mu}_{i_1}(t_1)||\hat{\mu}_{i_2}(t_2)||\hat{\mu}_{i_3}(t_2)| = |\hat{\mu}_{i_1}(t_2)||\hat{\mu}_{i_2}(t_1)||\hat{\mu}_{i_3}(t_1)|, \tag{14}$$

where all i_j are pairwise different.

Put $\nu_i = \mu_i * \bar{\mu}_i, i = 1, 2, \ldots, n$. Then $\hat{\nu}_i(y) = |\hat{\mu}_i(y)|^2, y \in Y$. The functions $\hat{\nu}_i(y)$ are nonnegative and also satisfy equation (3). It suffices to show that $\hat{\nu}_i(y)$ are characteristic functions of the idempotent distributions. This implies that $\hat{\mu}_i(y)$ are also characteristic functions of the idempotent distributions.

Now we will show that $N_i = N, i = 1, 2, 3$. Assume the converse. Then there exists $y_1 \in N_{i_1}$ such that either $y_1 \notin N_{i_2}$ or $y_1 \notin N_{i_3}$, where all i_j are pairwise different. Put $t_1 = y_1, t_2 = y_2$, where $y_2 \in N$ and y_1,y_2 belong to the same coset of $Y^{(2)}$ in Y, in (14). We can make such a choice. Indeed, on the one hand, $N \cap Y^{(2)} \neq \{0\}$ because N is a subgroup and $N \neq \{0\}$ by the assumption. On the other hand, there exists $y \neq 0$ such that $y \in N \cap (\tilde{y} + Y^{(2)})$. Indeed, if $N \subset Y^{(2)}$, then, taking into account (13), we infer that there exists $y' \in Y$ such that $y = 2^k y'$. This contradicts to the fact that there are no $y \in Y$ such that y is infinitely divisible by 2. We infer that the left-hand side of Eq. (14) is equal to a positive number, and the right-hand side of Eq. (14) is equal to zero. This is a contradiction. So we have that $N_i = N, i = 1, 2, 3$.

Note that if $y \in N$, then $\hat{\nu}_i(y) = 1,\ i = 1, 2, 3$. Indeed, let $y_0 \in N$. Consider the subgroup H of Y generated by y_0. Note that $H \cong \mathbb{Z}$. Consider the restriction of Eq. (3) to the subgroup H. Using Corollary 3.5, we obtain that $\hat{\nu}_i(y) = 1, i = 1, 2, 3, y \in H$.

Taking into account that the characteristic functions $\hat{\nu}_i(y)$ are N-invariant, consider the equation induced by equation (3) on the factor-group Y/N. Put $f_i([y]) = \hat{\nu}_i([y])$. Note that if H is an arbitrary nontrivial subgroup of Y, then Y/H is topologically isomorphic to a group of the form $\mathbf{P}^*_{p\in\mathcal{P}}\mathbb{Z}(p^{k_p})$, where $k_p \geq 0$.

In particular, this holds for the factor-group Y/N. Hence, by Corollary 3.3, we can conclude that $f_i([y])$ are characteristic functions of some idempotent distributions. This implies that all distributions μ_i are idempotent.

B. Consider the case $N = \{0\}$.

First putting $u_2 = 0, u_3 = u_1 = y$, then $u_3 = 0, u_1 = u_2 = y$, and finally $u_1 = 0, u_2 = u_3 = y$ in (3), we get respectively:

$$\hat{\mu}_1(2y) = \hat{\mu}_1^2(y)|\hat{\mu}_2(y)|^2|\hat{\mu}_3(y)|^2, \quad y \in Y. \tag{15}$$

$$\hat{\mu}_2(2y) = |\hat{\mu}_1(y)|^2\hat{\mu}_2^2(y)|\hat{\mu}_3(y)|^2, \quad y \in Y. \tag{16}$$

$$\hat{\mu}_3(2y) = |\hat{\mu}_1(y)|^2|\hat{\mu}_2(y)|^2\hat{\mu}_3^2(y), \quad y \in Y. \tag{17}$$

Note that

$$\hat{\mu}_i(2y) = 0, y \in Y, y \neq 0, i = 1, 2, 3. \tag{18}$$

Indeed, if $\hat{\mu}_{i_0}(2y_0) \neq 0$ for some $y_0 \in Y, y_0 \neq 0$, and i_0, then from Eqs. (15)–(17) it follows that $\hat{\mu}_i(y_0) \neq 0, i = 1, 2, 3$. This contradicts to $N \neq \{0\}$.

Show that at least one distribution $\mu_i = m_X$. Assume the converse. Then there exists $t_1 \neq 0, t_2 \neq 0, t_3 \neq 0$ such that

$$\hat{\mu}_1(\pm t_1)\hat{\mu}_2(\pm t_2)\hat{\mu}_3(\pm t_3) \neq 0. \tag{19}$$

From equality (18) it follows that $t_i \in \tilde{y} + Y^{(2)}$. From $N = \{0\}$ it follows that $\pm t_i, i = 1, 2, 3$, do not coincide. Without loss of generality, assume that $t_1 \neq \pm t_2$. Note that for all elements $y', y'' \in \tilde{y} + Y^{(2)}$ we have $y' + y'' \in Y^{(2)}$. Moreover, for any two elements $y', y'' \in \tilde{y} + Y^{(2)}$ there are two possibilities: either $y' + y'' \in Y^{(4)}$ or $y' - y'' \in Y^{(4)}$.

Put $y_i = t_i, i = 1, 2, 3$, if $t_1 + t_2 \in Y^{(4)}$, and put $y_1 = t_1, y_2 = -t_2, y_3 = t_3$ if $t_1 - t_2 \in Y^{(4)}$. Note that $y_1 + y_2 \in Y^{(4)}, y_1 + y_2 \neq 0$. For an element $y_0 \in Y^{(2)}$ denote by $\frac{y_0}{2}$ an element of Y such that $2\frac{y_0}{2} = y_0$. Thus we have that $\frac{y_1+y_2}{2} \in Y^{(2)}, \frac{y_1+y_2}{2} \neq 0$.

Consider the system of the equations

$$\begin{cases} u_1 + u_2 + u_3 = y_1, \\ u_1 - u_2 - u_3 = y_2, \\ u_1 + u_2 - u_3 = y_3. \end{cases} \tag{20}$$

Taking into account that $y_i \in \tilde{y} + Y^{(2)}, i = 1, 2, 3$, it is easy to see that the system of equations (20) has the following solutions:

$$\begin{cases} u_1 = \frac{y_1+y_2}{2}, \\ u_2 = \frac{y_3-y_2}{2}, \\ u_3 = \frac{y_1-y_3}{2} \end{cases} \tag{21}$$

Put the solutions of (21) in Eq. (3). Taking into account (19), we infer that the right-hand side of (3) is not equal to 0. This implies that

$$\hat{\mu}_1\left(\frac{y_1+y_2}{2}\right)\hat{\mu}_2\left(\frac{y_3-y_2}{2}\right)\hat{\mu}_3\left(\frac{y_1-y_3}{2}\right)\neq 0. \tag{22}$$

It follows from inequality (22) that $\mu_1(\frac{y_1+y_2}{2})\neq 0$. However, we have $\frac{y_1+y_2}{2}\in Y^{(2)}$, which contradicts to (18).

Note that we have also proved that if $N\neq\{0\}$, then all distributions μ_i are idempotent, and if $N=\{0\}$, then at least one distribution μ_i is the Haar distribution on X.

2. Now consider the case $f_p\in Aut(X)$ for some prime p. If $f_2\in Aut(X)$, then the statement follows from Lemma 3.8. Assume that $f_2\notin Aut(X)$. Then two cases, $p-1=4k$ and $p+1=4k$, are possible. Let us study the first case.

Consider the function $\rho(x)$ on X defined by the equation

$$\rho(x)=1+Re(x,y_0),$$

where $y_0\in Y, y_0\notin Y^{(2)}$. It is obvious that $\rho(x)\geq 0, x\in X$, and $\int_X\rho(x)dm_X(x)=1$. Let μ be a distribution on X with the density $\rho(x)$ with respect to m_X. It is also obvious that $\mu\notin\Gamma(X)*I(X)$. The characteristic function of the distribution μ is of the form

$$\hat{\mu}(y)=\begin{cases}1, & y=0,\\ \frac{1}{2}, & y=\pm y_0,\\ 0, & y\notin\{0,y_0,-y_0\}.\end{cases} \tag{23}$$

Let $\xi_i, i=1,2,3$, be independent identically distributed random variables with values in X and distribution μ. Let us verify that the linear forms $L_1=\xi_1+\xi_2+\xi_3, L_2=\xi_1+p\xi_2+\xi_3, L_3=\xi_1+\xi_2+p\xi_3$ are independent. By Lemma 3.1, it suffices to prove that $\hat{\mu}(y)$ satisfies Eq. (2), which takes the form

$$\hat{\mu}(u+v+t)\hat{\mu}(u+pv+t)\hat{\mu}(u+v+pt)=\hat{\mu}^3(u)\hat{\mu}^2(v)\hat{\mu}^2(t)\hat{\mu}(pv)\hat{\mu}(pt), \tag{24}$$

where $u,v,t\in Y$. We will show that Eq. (24) holds. Certainly it suffices to consider the case where at least two of three elements u,v,t are not equal to 0. It is easy to see that in this case the right-hand side of Eq. (24) is equal to 0. Let us show that the left-hand side of Eq. (24) is also equal to 0.

Suppose that there are some elements u,v,t such that the left-hand side of Eq. (24) does not vanish. Then there exist $h_i\in\{0,y_0,-y_0\}, i=1,2,3$, such that u,v,t satisfy the system of the equations

$$\begin{cases}u+v+t=h_1,\\ u+pv+t=h_2,\\ u+v+pt=h_3.\end{cases} \tag{25}$$

From (25), it is easy to obtain

$$(p-1)v, (p-1)t \in \{0, \pm y_0, \pm 2y_0\}. \tag{26}$$

Relationship (26) fails because $(p-1) = 4k$, but $y_0 \notin Y^{(2)}$. From this it follows that the left-hand side of equation (24) is equal to 0.

The second case can be studied in a similar way, but we have to consider the linear forms $L_1 = \xi_1 + \xi_2 + \xi_3, L_2 = \xi_1 - p\xi_2 + \xi_3, L_3 = \xi_1 + \xi_2 - p\xi_3$.

The theorem is completely proved. ■

References

[1] *G.M. Feldman*, On the Skitovich–Darmois Theorem for Finite Abelian Groups. — *Theory Probab. Appl.* **37** (1992), 621–631.

[2] *G.M. Feldman and P. Graczyk*, On the Skitovich–Darmois Theorem on Compact Abelian Groups. — *J. Theory Probab.* **13** (2000), 859–869.

[3] *G.M. Feldman*, On a Characterization Theorem for Locally Compact Abelian Groups. — *Probab. Theory Relat. Fields* **133** (2005), 345–357.

[4] *G.M. Feldman and P. Graczyk*, On the Skitovich–Darmois Theorem for Discrete Abelian Groups. — *Theory Probab. Appl.* **49** (2005), 527–531.

[5] *G.M. Feldman and M. Myronyuk*, On the Skitovich–Darmois Equation in the Classes of Continuous and Measurable Functions. — *Aequationes Mathematicae* **75** (2008), 75–92.

[6] *G.M. Feldman*, Independent Linear Statistics on $\boldsymbol{a}$-Adic Solenoids. — *Theory Probab. Appl.* **54** (2010), No. 3, 375–388.

[7] *G.M. Feldman*, Functional Equations and Characterizations Problems on Locally Compact Abelian Groups. — *EMS Tracts in Mathematics* **5** (2008), Zurich, European Mathematical Society (EMS).

[8] *G.M. Feldman and M. Myronyuk*, Independent Linear Statistics on the Cylinders. arXiv:1212.2772v1, 2012.

[9] *A.M. Kagan, Yu.V. Linnik, and C. Radhakrishna Rao*, Characterization Problems in Mathematical Statistics. *Wiley Series in Probability and Mathematical Statistics* Wiley, New York, 1973.

[10] *I.P. Mazur*, The Skitovich–Darmois Theorem for Finite Abelian Groups (the case of n linear forms of n random variables). — *U.M.J.* **4** (2011), 1512–1523.

[11] *I.P. Mazur*, The Skitovich–Darmois Theorem for Discrete and Compact Totally Disconnected Abelian Groups. arXiv:1112.1488v1, 2011.

[12] *E. Hewitt and A. Ross*, Abstract Harmonic Analysis, Vol. 1. Springer–Verlag, Berlin, Gottingen, Heildelberg, 1963.

[13] *K.R. Parthasarathy*, Probability Measures on Metric Spaces Chelsea Publishing (AMS), 1967.